Abstract

A process is described which can be used to generate a cryptographic key for a group of subscribers whose number is subject to change. The process can further provide that even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

Abstract

The process is to be such that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

According to the present invention, each of the n subscribers (I) is assigned to one leaf of a binary-structured tree which has precisely n leaves and is of depth $\lceil \log_2 n \rceil$. For each subscriber (I), a secret (i) is generated and is assigned to that leaf of the tree to which the respective subscriber (I) is also assigned. Secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, two already known secrets always being combined via the DH process to form a new common secret. The last node K_w contains the common key of all n subscribers.

The process of the present invention can be advantageously used to generate a cryptographic key for a group of subscribers whose number is subject to change.

Fig. 1